OPEN EN VEILIG SAMENWERKEN

Contextgebaseerde toegang en identiteitdifferentiatie

Toegang tot zakelijke informatie verloopt nog altijd op basis van iemands identiteit en autorisaties. Authenticatie bepaalt hierbij of iemand daadwerkelijk is wie hij of zij aangeeft te zijn. Het traditionele beeld waarbij alle informatie veilig achter een centrale bedrijfsfirewall beschermd is, vervaagt en binnen en buiten wordt steeds meer een vloeiende overgang. Bedrijven, overheidsinstellingen en zeker onderzoeks- en onderwijsinstellingen gaan steeds intensiever samenwerken met elkaar in ketens en netwerken.

Thuiswerken of onderweg werken in het kader van het nieuwe werken met zakelijke maar ook privéapparatuur is tegenwoordig normaal (BYOD). Ook lopen privé en zakelijke werkzaamheden steeds vaker door elkaar heen en het wordt steeds moeilijker om deze te scheiden. Zakelijke apparaten en informatiesystemen worden voor privédoelen gebruikt en vice versa. Hierbij lopen digitale identiteiten ook deels door elkaar heen. Het Facebook-account wordt maar al te makkelijk ook gebruikt om op een zakelijk forum in te loggen. Nieuwe medewerkers en studenten vinden het makkelijk om hun bestaande digitale identiteit te gebruiken om toegang tot informatie te krijgen. BYOI (Bring your own identity) is de trend. Waarom heb je als student nog een Universiteitsaccount nodig als je ook met je Gmail zou kunnen inloggen is de beleving. Daarnaast volgen studenten steeds vaker onderwijs bij verschillende universiteiten in het binnen- en buitenland. MOOCs (Massive Open Online Courses) worden steeds populairder en gaan meetellen voor studiepunten. Ook hierbij speelt de uitdaging voor de student welke digitale identiteit gebruikt wordt voor deelname aan deze vorm van onderwijs.

Het gebruik van cloud-oplossingen neemt snel toe binnen de onderzoeks- en onderwijswereld. Docenten en onderzoekers zijn vanuit privésituaties gewend om zelf te kiezen welk systeem het beste werkt en willen ook op het werk kunnen kiezen welke systemen ze gebruiken. Daarnaast zijn vaak hele specifieke en innovatieve nieuwe systemen nodig voor het onderzoek en onderwijs. Het gebruik van deze systemen wordt vaak buiten de IT-organisatie om afgenomen in de cloud. Hierbij maakt men meestal gebruik van nieuwe accounts en wachtwoorden. Vaker dan gedacht worden hierbij bedrijfswachtwoorden hergebruikt met alle risico's van dien. Federatieve toegang vanuit een centrale identity-provider zou hier een oplossing voor kunnen bieden.

Maar ook de wereld van smartphones en tablets met apps levert nieuwe uitdagingen op. Hoe vindt hier authenticatie plaats en zeker als twee-factor-authenticatie vereist is.

Vanuit het informatiebeveiligingsbeleid proberen veel organisaties doormiddel van informatieclassificatie top-down grip te krijgen op de minimale beveiligingseisen en gebruiksvoorwaarden voor een bepaalde informatieclassificatie. Voor toegang tot geheime informatie wordt steeds vaker een tweede factor vereist (2FA of MFA multi-factor-authenticatie) naast het traditionele wachtwoord dat zijn langste tijd gehad heeft [1] [2].
Social-engineering-aanvallen middels phishing-mails zijn namelijk effectief genoeg gebleken (rond de 10% geeft wachtwoord af op basis van een matige phishing mail) om accounts te compromitteren. Spionage dat volgens de AIVD een reëel risico voor kennisintensieve sectoren binnen Nederland [3] en overlast (o.a. spamruns) zijn het gevolg maar ook vaak de aanleiding voor extra beveiligingsmaatregelen. Aan de andere kant willen medewerkers makkelijk anytime anyplace anywhere bij de informatie kunnen. Maak je het de gebruiker te moeilijk dan worden creatieve work-arounds bedacht (denk aan forwarden mails, syncen van folders naar cloud-oplossingen, delen van wachtwoorden, et cetera).

Open en veilig tegelijk is een must

Onderwijs- en onderzoeksinstellingen (maar algemener alle kennisinstellingen) staan voor de uitdaging om enerzijds hun intellectueel eigendom passend te beschermen maar anderzijds heel nauw samen te werken met alle soortige partijen en personen. Kortweg hoe realiseer ik open en veilige samenwerking? Hoe blijf ik "in control" over onze informatie en identiteiten?

Het simpelweg invoeren van twee-factor-authenticatie voor informatiesystemen met vertrouwelijke en geheime informatie zal tot weinig draagvlak en mogelijk zelfs weerstand leiden (de cultuur is principieel anders dan bij een bank bijvoorbeeld). Gebruikers zouden mogelijk hun werkplek niet vergrendelen om maar niet opnieuw te hoeven inloggen en bestanden op andere plekken neer gaan zetten (dan wel uit systemen halen). De beste resultaten worden behaald indien de gebruiker snapt

Raoul Vernède is security officer bij Wageningen University & Research. Raoul is te bereiken via raoul.vernede@wur.nl.

wanneer een tweede factor voor authenticatie redelijkerwijs vereist is naast het wachtwoord. Op die manier is draagvlak en begrip te krijgen. Een gebruiker zal begrip hebben dat een tweede factor nodig is indien vanuit de trein met een eigen apparaat vertrouwelijke zakelijke informatie wordt geraadpleegd. Men heeft weinig begrip indien men vanaf de eigen werkplek met een beheerd apparaat dezelfde informatie benadert in een systeem dat een half uur geleden ook al benaderd is.
Om dit te kunnen realiseren is context en risk-gebaseerde authenticatie nodig [4]. Hierbij wordt, gebruikmakend van een aantal criteria bepaald of, en onder welke voorwaarden, (enkel wachtwoord of aangevuld met tweede factor) men toegang krijgt.

Het bovenstaande overzicht laat deze verschuiving ook goed zien van de klassieke naar een modernere benadering van IAM [5]. Traditioneel gezien zijn (onderwijs- en onderzoeks-) instellingen goed georganiseerd in identiteitenbeheer maar ligt er minder focus op toegangsbeheer (access management).

Naast aanvullende authenticatie (het stukje veilig samenwerken) is het nodig om na te denken hoe makkelijker samengewerkt kan worden met externe personen (het stukje open in de samenwerking). Hiertoe moet onderscheid gemaakt gaan worden in meer verschillende identiteiten met elk hun eigen trustlevel (differentiatie van identiteiten) op basis van Level of Assurance. Een eigen medewerker die een formeel HRM-proces doorlopen heeft met een fysieke check tussen paspoort en persoon een veel hoger vertrouwensniveau dan iemand die enkel bekend is van een e-mailadres zonder aanvullende validatie. Het Level of Assurance [6] verschilt daardoor per identiteit.

Trustlevel raamwerk

Een visie is nodig om deze open en veilige toegang en samenwerking te realiseren. Hiertoe is onderstaand raamwerk uitgewerkt en is Wageningen University & Research momenteel bezig dit te implementeren met het product van SecureAuth. Verschillende interne informatiesystemen (service providers) worden via het SAML v2 claim-based-protocol gekoppeld aan de on-premise SecureAuth IDP. SAML is een verplichte overheidsstandaard (pas toe leg uit) [7]. Deels zijn deze service-providers momenteel via SAML aan Microsoft ADFS gekoppeld.

Centrale insteek hierbij is trust in diverse context gerelateerde aspecten. De werkelijkheid vertoont steeds meer gradaties en het integrale niveau van deze factoren bepaald met behulp van decisions rules in de centrale IDP (identity provider) de toegang. Deze aanpak maakt inrichting veel complexer maar zorgt er wel voor dat toegang veel fijnmaziger ingeregeld kan worden. Gebruikersacceptatie stijgt hierdoor voor de inzet van twee-factor-authenticatie.

De volgende trustlevels worden onderscheiden: information, device, identity, network en authentication. Hieronder worden deze nader uitgewerkt en toegelicht (in oplopend niveau van vertrouwen). Algemeen is het advies om het aantal niveaus beperkt te houden. Later verder differentiëren kan makkelijker en het risico op het zich verliezen in details en complexiteit is groot.

1. Trustlevel information

Het gaat hierbij om de classificatie van de informatie ten aanzien van integriteit en vertrouwelijkheid. Veel organisaties classificeren de bedrijfsinformatie in 4 of meer klassen. Per classificatie wordt aangeven of authenticatie met een wachtwoord dan wel 2FA vereist is.

- Openbaar
- Intern
- Vertrouwelijk (inclusief alle persoonsgegevens)
- Geheim

2. Trustlevel device

Het gaat hierbij om het vertrouwen dat je als organisatie hebt in het beveiligingsniveau en bekendheid van het apparaat waarmee de informatie benaderd wordt.

- Onbekend apparaat (denk aan toegang vanaf internetcafécomputers)
- Herkend en dus (recent) reeds eerder gezien apparaat (wordt door profiling/finger printing van de browser bepaald

op basis van een divers aantal kenmerken). Binnen SecureAuth heet dit UBC (Universal Browser Credential)
- Bekend apparaat op basis van user-certificaat (X509) dat door de gebruiker geplaatst is (hierbij geeft de gebruiker aan dit apparaat te vertrouwen is. Certificaat kan enkel gedownload worden na succesvolle twee-factor-authenticatie)
- Geregistreerd apparaat via een formeel MDM (mobile device management) proces waarbij bijvoorbeeld MDM-agent geplaatst wordt op het BYOD (via MDM-tooling kan deels bepaalde beveiliging van het apparaat afgedwongen worden zoals up-to-date virusscanner en bepaalde policies)
- Geheel beheerd (fysiek/virtueel) apparaat waardoor uitgebreide beveiligingseisen afgedwongen kunnen worden (meestal uitsluitend voor gebruikers en apparatuur die gekoppeld zijn aan de enterprise-directory). Vaak is een organisatie eigen CA/PKI-device-certificaat op het apparaat geïnstalleerd. Deze categorie omvat zowel fysieke als ook virtueel apparaat (VDI of remote deskop).

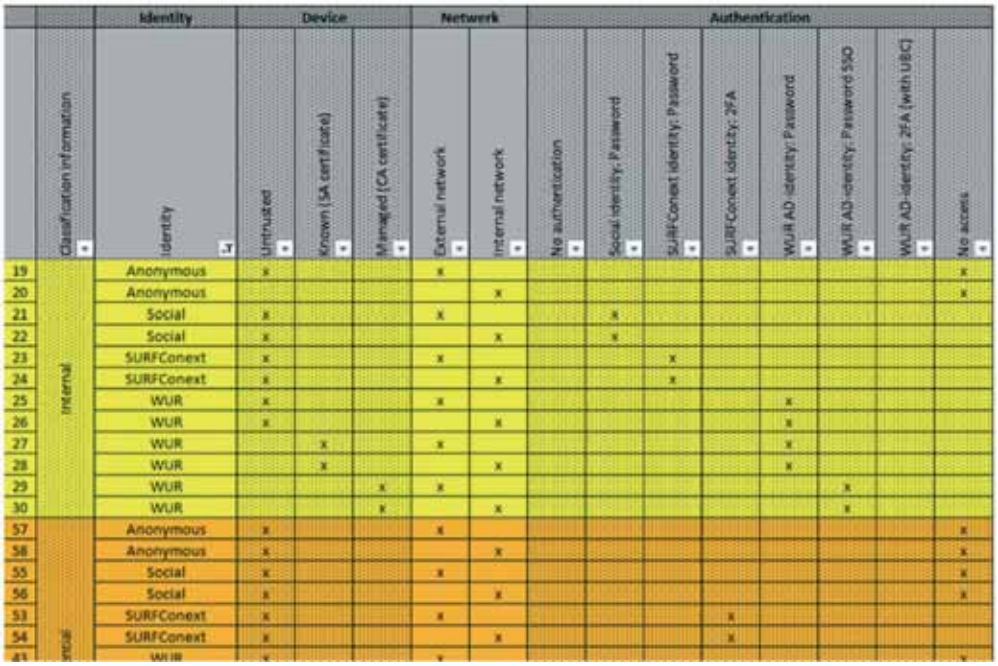
3. Trustlevel identity

Dit betreft het niveau van vertrouwen wat men in de (gevalideerde) identiteit van een gebruiker heeft. Ofwel hoe zeker kan ik zijn dat de identiteit klopt. Hierbij gaat het om bedrijfsinterne dan wel externe gebruiker directories.
- Anoniem; identiteit zoals een bezoeker aan een website.
- Sociaal gefedereerd; gebruiker waarbij identiteit enkel via e-mailverificatie heeft plaats gevonden. De eigenaar heeft toegang tot een bepaald sociaal (bijvoorbeeld Facebook of Linkedin) of e-mail-account (bijvoorbeeld Gmail of Hotmail). Vergelijkbaar met een eigen bedrijfseigen database met enkel e-mailvalidatie.
- Partner en/of sector gefedereerd; gebruikers waarbij er van uit gegaan wordt dat voor partners dan wel communities (zoals de SURF-federatie voor onderzoek en onderwijs) een vergelijkbaar aan de eigen organisatie robuust HRM-registratieproces aanwezig is.
- Eigen identiteit; (meestal in enterprise directory); Identiteit van medewerkers op basis van robuust HRM registratieproces met fysieke check op identiteit.

4. Trustlevel network

Vanuit welk netwerk of zone/segment wordt de informatie benadert. Vaak op basis van IP-ranges.
- Intern bedrijfsnetwerk eventueel nog verbijzonderd naar trusted of semi-trusted (DMZ-)segment.
- Extern netwerk (buiten de firewall) en daardoor onbekend en untrusted.

Authentication matrix Wageningen UR



		Identity	Device			Network		Authentication							
	Classification information	Identity	Untrusted	Known (SA certificate)	Managed (CA certificate)	External network	Internal network	No authentication	Social identity: Password	SURFconext identity: Password	SURFconext identity: 2FA	WUR AD -identity: Password	WUR AD-identity: Password SSO	WUR AD-identity: 2FA (with UBC)	No access
19	internal	Anonymous	x			x									x
20	internal	Anonymous					x								x
21	internal	Social	x			x			x						
22	internal	Social	x				x		x						
23	internal	SURFConext	x			x				x					
24	internal	SURFConext	x				x			x					
25	internal	WUR	x			x						x			
26	internal	WUR	x				x					x			
27	internal	WUR		x		x						x			
28	internal	WUR		x			x					x			
29	internal	WUR			x	x							x		
30	internal	WUR			x		x						x		
57	external	Anonymous	x			x									x
58	external	Anonymous	x				x								x
55	external	Social	x			x									x
56	external	Social	x				x								x
53	external	SURFConext	x			x					x				
54	external	SURFConext	x				x				x				
43	external	WUR	x			x									x

5. Trustlevel authentication

Het gaat hierbij om het niveau van vertrouwen in een bepaalde manier van authenticatie van een gebruiker (identiteit).

- o Geen authenticatie is nodig.
- o Wachtwoord van een gefedereerd sociaal of e-mailaccount.
- o Wachtwoord van een partner en/of sector gefedereerde gebruiker.
- o Wachtwoord van eigen identiteiten (medewerker accounts) (gelijkwaardig aan SSO-Kerberos-ticket).
- o Wachtwoord en 2FA van partner en/of sector gefedereerde gebruiker. Hierbij wordt de 2FA-inrichting van de andere organisatie vertrouwd en kan de gefedereerde gebruiker met zijn eigen 2FA-methode authentiseren. SAML-protocol afspraken tussen de federatieve organisaties dienen gemaakt te worden.
- o Wachtwoord en 2FA van eigen identiteiten.

Op basis van bovenstaande trustlevels kunnen nu voor elke combinatie beslisregels opgesteld worden. Hierboven een voorbeeld van een deel van deze regels (die voor elke organisatie er anders uit zullen zien). Het zijn in feite een aantal geneste als- dan vragen. Aansluitend kan per service-provider op basis van de informatieclassificatie de toegangsregels geïmplementeerd worden in de IDP. Aanvullend op bovenstaande kunnen ook zaken als overlast door identiteitendiefstal een rol spelen (denk aan spamruns).

Aandachtspunten

Diverse leveranciers van IAM - web-access-management-tooling hebben of zijn momenteel bezig contextgebaseerde toegang in hun producten op de een of andere manier te implementeren [8][9]. Wageningen University & Research is momenteel bezig SecureAuth te implementeren op basis van het eerder geschetste raamwerk. Er zijn een aantal zaken opgevallen die aandacht behoeven.

Contextgebaseerde authenticatie via een centrale IDP is een flinke stap vooruit maar het probleem van de provisioning van accounts of identiteiten naar de verschillende (cloud) service providers is daarmee niet opgelost. Met name voor het autoriseren van gebruikers voor bijvoorbeeld toekennen van rechten of licenties vereisen veel cloud providers dat identiteiten worden geprovisoned. Bij een federatieve oplossing waarbij de identiteiten in eigen beheer zijn is wel het risico van oneigenlijke toegang na vertrek verminderd omdat de betreffende account zich niet meer kunnen authentiseren (ondanks dat de identiteit nog aanwezig is bij de service provider). Via regelmatige synchronisatie met de eigen enterprise directories kan dit voorkomen worden. Dit laatste levert in veel gevallen ook een besparing op in onnodige licentie kosten.

Denk na over wie binnen je organisatie verantwoordelijk is voor externe gebruikers die via sociale of email accounts dan wel gefedereerd toegang krijgen tot bedrijfsinformatie. Regel je dit centraal of laat je dit over aan de medewerkers zelf en wat gebeurt er bij overlast of zelfs misbruik. Welke juridische relatie heb je dan als organisatie met zo'n gebruiker. Maakt men gebruik van een eigen database voor externe gebruikers dan zal nagedacht moeten worden over het opschonen van gebruikers.

Overweeg na een succesvolle introductie van 2FA of een eventuele eis vanuit het wachtwoordenbeleid voor het veranderen van wachtwoorden kan worden verlicht. Veranderen van wachtwoorden is vervelend voor gebruikers en levert zeker in combinatie met 2FA weinig toegevoegde waarde. Misschien is het voldoende om wachtwoorden enkel 1 keer jaar te veranderen! [10]

Veel oudere of niet webgebaseerde diensten ondersteunen nog geen SAML v2 protocol. In de veel gevallen is het ook gewenst om deze diensten ook via 2FA te ontsluiten. Denk hierbij aan VPN-connecties met behulp van legacy Radius-systemen of client-server-applicaties. Contextgebaseerde 2FA is hier lastiger dan voor web-based-applicaties. Bijzondere grote uitdaging ligt hier bij e-mailsystemen die gebruik maken van Active Sync of Pop3. Voor dergelijke protocollen zijn nauwelijks alternatieven of oplossingen beschikbaar terwijl ze gelijktijdig breed en veel gebruikt worden op eigen en privéapparatuur. Client-server-applicaties kunnen vaak wel gevirtualiseerd worden, zodat ze over HTTPS gestart kunnen worden.

Door het inrichten van een centrale (eventueel on premise) IDP met decisions rules en het afdwingen van SAML ondersteunde cloud-diensten in het IT-inkoopproces, krijgt men als organisatie meer regie op schaduw-IT. Voor cloudsysteemeigenaren is makkelijke maar ook veilige toegang belangrijk en daarin kan een centrale IDP ondersteuning bieden.

De genoemde context factoren zoals eerder genoemd zijn zeker geen eindstation. Deze zullen de komende tijd verder uitgebreid en verfijnd worden met andere factoren. De stap zal tevens gezet worden naar continuous authentication met behulp van bijvoorbeeld karakteristieken van de toetsaanslag en muisbewegingen van gebruikers (behavioral biometrics) [11].

Denk goed na hoe het initiële enrolment-proces van 2FA er uit moet zien. Gaat men werken met fysieke tokens of soft tokens zoals sms of app. Indien met soft tokens gewerkt gaat worden, hoe kunnen dan nieuwe telefoonnummers gekoppeld worden? Dit moet enkel kunnen na een 2FA-validatie van de gebruiker (bijvoorbeeld op basis van een niet te wijzigen mobiel nummer dat gekoppeld is via het HRM-proces aan een medewerker, deze persoon heeft dan een hoog level of assurance).

Step-up-authenticatie binnen dezelfde applicatie voor specifieke handelingen met hogere authenticatie eisen (bijvoorbeeld invoeren van cijfers in studenten informatiesysteem versus enkel raadplegen van cijfers), is enkel mogelijk indien de applicatie dit ondersteunt. Er dient dan een nieuw verzoek naar de IDP te gaan voor een aanvullende authenticatie met 2FA.

Indien applicaties niet voorzien in mogelijkheden om bevoegdheden te delegeren tijdens afwezigheid van de medewerkers, worden ondanks dat dit niet gewenst is, gebruikersnaam en wachtwoord aan de secretaresse of collega gegeven. Deze persoon kan dan namens de afwezige persoon bijvoorbeeld uren of kosten fiatteren. Bij gebruik van 2FA zal deze traditionele aanpak niet meer mogelijk zijn en hier moet rekening mee gehouden worden tijdens de implementatie van 2FA.

Maakt men als organisatie veel gebruik van apps voor mobiele platformen dan zal nagedacht moeten worden hoe 2FA hierin past. De apps dienen 2FA native te ondersteunen. Vaak wordt gebruik gemaakt van het OAuth-protocol. Een optie is het gebruik van een mobiele app portal waarop eenmalig moet worden ingelogd met 2FA.

De technologische ontwikkelingen gaan snel en er is veel dynamiek in de IAM wereld. Technologieën zijn nog niet uitgekristalliseerd en de complexiteit neemt toe. Dit vraagt om visie en lef om toch stappen te gaan zetten als (IT-)organisatie. Start nu om veilige en open samenwerking mogelijk te maken. Think big, Act small.

Links

[1] NCSC Factsheet Gebruik Tweefactorauthenticatie, 2015. https://www.ncsc.nl/actueel/factsheets/factsheet-gebruik-tweefactorauthenticatie.html

[2] User Authentication Technologies Beyond the Password. Anne Elizabeth Robins & Trent Henry –Gartner 2015.

[3] Rapport Cyberbedreigingsbeeld Sector Hoger Onderwijs en Wetenschappelijk Onderzoek – SURF 2015.

[4] Enterprise Adaptive Access: Are We There Yet? Mark Diodati & Trent Henry - Gartner, 2015.

[5] http://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2014/report-idmaas-jan2014-def.pdf

[6] https://wiki.surfnet.nl/display/surfconextdev/Levels+of+Assurance

[7] https://www.forumstandaardisatie.nl/standaard/saml

[8] Magic Quadrant for User Authentication. Ant Allan, Anmol Singh & Eric Ahlm -Gartner, 2014

[9] Market Guide for Web Access Management Software. Gregg Kreizman, Gartner, 2015

[10] http://arstechnica.com/security/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/

[11] https://www.secureauth.com/IdP/Authentication-Security/Adaptive-Authentication/Behavioral-Biometrics.aspx